Foundation of Cryptography, Lecture 7
Commitment Schemes

Iftach Haitner, Tel Aviv University

Tel Aviv University.

May 7, 2013

Section 1

Commitment Schemes

Commitment Schemes

Digital analogue of a safe.

Commitment Schemes

Digital analogue of a safe.

Definition 1 (Commitment scheme)

An efficient two-stage protocol (S, R) .

Commit The sender S has private input $\sigma \in \{0,1\}^*$ and the common input is 1^n. The commitment stage results in a joint output c, the commitment, and a private output d to S, the decommitment.

Reveal S sends the pair (d, σ) to R, and R either accepts or rejects.

Completeness: R always accepts in an honest execution.

Commitment Schemes

Digital analogue of a safe.

Definition 1 (Commitment scheme)

An efficient two-stage protocol (S,R) .

Commit The sender S has private input $\sigma \in \{0,1\}^*$ and the common input is 1^n. The commitment stage results in a joint output c, the commitment, and a private output d to S, the decommitment.

Reveal S sends the pair (d,σ) to R, and R either accepts or rejects.

Completeness: R always accepts in an honest execution.

Hiding:. In commit stage: $\forall$ PPT R^*, $m \in \mathbb{N}$ and $\sigma \neq \sigma' \in \{0,1\}^m$, $\{\mathsf{View}_{\mathsf{R}^*}(\mathsf{S}(\sigma),\mathsf{R}^*)(1^n)\}_{n\in\mathbb{N}} \approx_c \{\mathsf{View}_{\mathsf{R}^*}(\mathsf{S}(\sigma'),\mathsf{R}^*)(1^n)\}_{n\in\mathbb{N}}$.

Commitment Schemes cont.

Binding: A cheating sender S^* succeeds in the following game with negligible probability in n:

> *On security parameter 1^n, S^* interacts with R in the commit stage resulting in a commitment c, and then output two pairs (d, σ) and (d', σ') with $\sigma \neq \sigma'$ such that $\mathsf{R}(c, d, \sigma) = \mathsf{R}(c, d', \sigma') = \texttt{Accept}$*

Commitment Schemes cont.

- wlg. we can think of d as the random coin of S, and c as the transcript

Commitment Schemes cont.

- wlg. we can think of d as the random coin of S, and c as the transcript
- Hiding: Perfect, statistical, computational

Commitment Schemes cont.

- wlg. we can think of d as the random coin of S, and c as the transcript
- Hiding: Perfect, statistical, computational
- Binding: Perfect, statistical. computational

Commitment Schemes cont.

- wlg. we can think of d as the random coin of S, and c as the transcript
- Hiding: Perfect, statistical, computational
- Binding: Perfect, statistical. computational
- Cannot achieve both properties to be statistical simultaneously.

Commitment Schemes cont.

- wlg. we can think of d as the random coin of S, and c as the transcript
- Hiding: Perfect, statistical, computational
- Binding: Perfect, statistical. computational
- Cannot achieve both properties to be statistical simultaneously.
- For computational security, we will assume non-uniform entities:

Commitment Schemes cont.

- wlg. we can think of d as the random coin of S, and c as the transcript
- Hiding: Perfect, statistical, computational
- Binding: Perfect, statistical. computational
- Cannot achieve both properties to be statistical simultaneously.
- For computational security, we will assume non-uniform entities:

  On security parameter n, the adversary gets an auxiliary input z_n (length of auxiliary input does not count for the running time)

Commitment Schemes cont.

- wlg. we can think of d as the random coin of S, and c as the transcript
- Hiding: Perfect, statistical, computational
- Binding: Perfect, statistical. computational
- Cannot achieve both properties to be statistical simultaneously.
- For computational security, we will assume non-uniform entities:

  On security parameter n, the adversary gets an auxiliary input z_n (length of auxiliary input does not count for the running time)
- Suffices to construct “bit commitments"

Commitment Schemes cont.

- wlg. we can think of d as the random coin of S, and c as the transcript
- Hiding: Perfect, statistical, computational
- Binding: Perfect, statistical. computational
- Cannot achieve both properties to be statistical simultaneously.
- For computational security, we will assume non-uniform entities:

  On security parameter n, the adversary gets an auxiliary input z_n (length of auxiliary input does not count for the running time)
- Suffices to construct “bit commitments"
- (non-uniform) OWFs imply statistically binding, and statistically hiding commitments

Perfectly Binding Commitment from OWP

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ be a permutation and let b be a (non-uniform) hardcore predicate for f.

Perfectly Binding Commitment from OWP

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ be a permutation and let b be a (non-uniform) hardcore predicate for f.

Protocol 2 ((S,R))

Commit:

S's input: $\sigma \in \{0,1\}$

S chooses a random $x \in \{0,1\}^n$, and sends $c = (f(x), b(x) \oplus \sigma)$ to R

Reveal:

S sends (x,σ) to R, and R accepts iff (x,σ) is consistent with c (i.e., $f(x) = c_1$ and $b(x) \oplus \sigma = c_2$)

Claim 3

Protocol 2 is perfectly binding and computationally hiding commitment scheme.

Proof:

Claim 3

Protocol 2 is perfectly binding and computationally hiding commitment scheme.

Proof: Correctness and binding are clear.

Claim 3

Protocol 2 is perfectly binding and computationally hiding commitment scheme.

Proof: Correctness and binding are clear.

Hiding: for any (possibly non-uniform) algorithm A, let

$$\Delta_n^{\mathsf{A}} = |\Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 0) = 1] - \Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 1) = 1]|$$

Claim 3

Protocol 2 is perfectly binding and computationally hiding commitment scheme.

Proof: Correctness and binding are clear.

Hiding: for any (possibly non-uniform) algorithm A, let

$$\Delta_n^{\mathsf{A}} = |\Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 0) = 1] - \Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 1) = 1]|$$

It follows that

$$|\Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 0) = 1] - \Pr[\mathsf{A}(f(U_n), b(U_n) \oplus U) = 1]| = \Delta_n^{\mathsf{A}}/2$$

Claim 3

Protocol 2 is perfectly binding and computationally hiding commitment scheme.

Proof: Correctness and binding are clear.

Hiding: for any (possibly non-uniform) algorithm A, let

$$\Delta_n^{\mathsf{A}} = |\Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 0) = 1] - \Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 1) = 1]|$$

It follows that

$$|\Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 0) = 1] - \Pr[\mathsf{A}(f(U_n), b(U_n) \oplus U) = 1]| = \Delta_n^{\mathsf{A}}/2$$

Hence,

$$|\Pr[\mathsf{A}(f(U_n), b(U_n)) = 1] - \Pr[\mathsf{A}(f(U_n), U) = 1]| = \Delta_n^{\mathsf{A}}/2 \tag{1}$$

Claim 3

Protocol 2 is perfectly binding and computationally hiding commitment scheme.

Proof: Correctness and binding are clear.
Hiding: for any (possibly non-uniform) algorithm A, let

$$\Delta_n^{\mathsf{A}} = |\Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 0) = 1] - \Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 1) = 1]|$$

It follows that

$$|\Pr[\mathsf{A}(f(U_n), b(U_n) \oplus 0) = 1] - \Pr[\mathsf{A}(f(U_n), b(U_n) \oplus U) = 1]| = \Delta_n^{\mathsf{A}}/2$$

Hence,

$$|\Pr[\mathsf{A}(f(U_n), b(U_n)) = 1] - \Pr[\mathsf{A}(f(U_n), U) = 1]| = \Delta_n^{\mathsf{A}}/2 \qquad (1)$$

Thus, Δ_n^{A} is negligible for any PPT

Statistically Binding Commitment from OWF.

Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{3n}$ be a (non-uniform) PRG

Statistically Binding Commitment from OWF.

Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{3n}$ be a (non-uniform) PRG

Protocol 4 ((S,R))

Commit Common input: 1^n.
S's input: $\sigma \in \{0,1\}$.

1. R chooses a random $r \leftarrow \{0,1\}^{3n}$ to S
2. S chooses a random $x \in \{0,1\}^n$, and send $g(x)$ to S in case $\sigma = 0$ and $c = g(x) \oplus r$ otherwise.

Reveal: S sends (σ, x) to R, and R accepts iff (σ, x) is consistent with r and c

Correctness is clear.

Statistically Binding Commitment from OWF.

Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{3n}$ be a (non-uniform) PRG

Protocol 4 ((S,R))

Commit Common input: 1^n.

S's input: $\sigma \in \{0,1\}$.

1. R chooses a random $r \leftarrow \{0,1\}^{3n}$ to S
2. S chooses a random $x \in \{0,1\}^n$, and send $g(x)$ to S in case $\sigma = 0$ and $c = g(x) \oplus r$ otherwise.

Reveal: S sends (σ, x) to R, and R accepts iff (σ, x) is consistent with r and c

Correctness is clear. Hiding and biding HW